B. AMENDMENTS TO CLAIMS

Please amend the claims as indicated hereinafter.

1. (CURRENTLY AMENDED) A multi-function peripheral device comprising:

a network interface configured to allow the multi-function peripheral device to communicate with network devices over a network;

a graphical user interface configured to allow for the exchange of information between the multi-function peripheral device and a user;

one or more processors;

a memory;

a scan process executing in the memory and being configured to cause a printed document to be scanned at the multi-function peripheral device and to generate scan data that includes a digital data representation of the electronic document;

a print process executing in the memory and being configured to process print data and cause a printed version of an electronic document reflected in the print data to be generated by the multi-function peripheral device at the multi-function peripheral device; and

a virus protection process executing in the memory and being configured to

detect that one or more unauthorized instructions have been stored on the multi-function peripheral device; and

in response to detecting that the one or more unauthorized instructions have been stored on the multi-function peripheral device, perform one or more actions to address the one or more unauthorized instructions that have been stored on the multi-function peripheral device.

2. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by periodically examining, according to specified configuration criteria, data stored on the multi-function peripheral device to determine whether the data has been modified in an unauthorized manner.

3. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting that one or more data files stored on the multi-function peripheral device have been modified.

4. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting that program code stored on the multi-function peripheral device has been modified.

5. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral device by examining and detecting that configuration data stored on the multi-function peripheral device has been modified.

6. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to examine data stored on a non-volatile memory of the multi-function peripheral device.

7. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is configured to examine data stored in a volatile memory of the multi-function peripheral device.

8. (ORIGINAL) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to undo changes made as a result of execution of the one or more unauthorized instructions.

9. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to

determine whether particular data stored on the multi-function peripheral device can be restored to a prior state; and

in response to determining that the particular data cannot be restored to the prior state, then delete the particular data from the multi-function peripheral device.

10. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to render the one or more unauthorized instructions inaccessible and unexecutable on the multi-function peripheral device.

11. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to notify a user via ~~a~~ the graphical user interface on the multi-function peripheral device that the storage of the one or more unauthorized instructions on the multi-function peripheral device has been detected.

12. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to notify a user by printing a report on the multi-function peripheral device that indicates that ~~the~~ storage of the one or more unauthorized instructions on the multi-function peripheral device has been detected.

13. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to provide notification via an email that ~~the~~ storage of the one or more unauthorized instructions on the multi-function peripheral device has been detected.

14. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the virus protection process is further configured to provide notification via a facsimile that ~~the~~ storage of the one or more unauthorized instructions on the multi-function peripheral device has been detected.

15. (CURRENTLY AMENDED) The multi-function peripheral device as recited in Claim 1, wherein the multi-function peripheral device is configured to receive, over a network, data used by the virus protection process to detect that the one or more unauthorized instructions have been stored on the multi-function peripheral.